PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-095991
(43)Date of publication of application : 08.04.1994

(51)Int.Cl. G06F 13/00

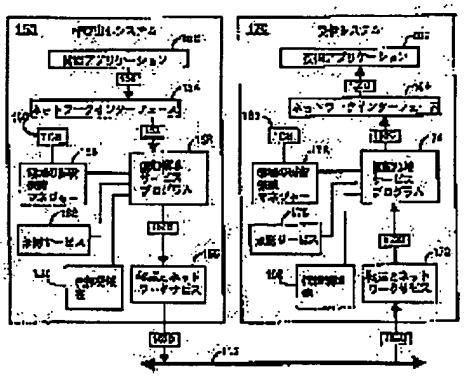
(21)Application number : 03-153021
(22)Date of filing : 25.06.1991

(71)Applicant : DIGITAL EQUIP CORP <DEC>
(72)Inventor : BARLOW DOUGLAS C

(30)Priority
Priority number : 90 543164 Priority date : 25.06.1990 Priority country : US

(54) DISTRIBUTED MULTI-LEVEL COMPUTER SECURITY SYSTEM AND METHOD FOR THIS SYSTEM

(57)Abstract:
PURPOSE: To provide a mechanism which secures communication in a reliable area of a system.
CONSTITUTION: Reliable area definition tables 130 and 182 define which reliable areas computers 150 and 170 are members of, and these tables define the security level of stored data. For the purpose of transmitting a designated message to the other computer system 170, a reliable area service program 156 checks that both of systems are members of a common reliable area and transmits the message as a protocol data unit. The reception system 170 verifies components of this data unit to discriminate which security policy should be executed for this message.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平6－95991

(43)公開日　平成6年(1994)4月8日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　13/00	３５１　Ｚ	7368－5B		

審査請求　有　　請求項の数3(全 11 頁)

(21)出願番号　特願平3－153021

(22)出願日　平成3年(1991)6月25日

(31)優先権主張番号　５４３１６４

(32)優先日　1990年6月25日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　590002873
ディジタル　イクイプメント　コーポレイション
アメリカ合衆国　マサチューセッツ州　01754メイナード　メイン　ストリート　146

(72)発明者　ダグラス　シー　バーロウ
アメリカ合衆国　ワシントン州　98053　レッドモンド　トゥーハンドレッドアンドセヴンティーンス　アベニュー　ノースイースト　308

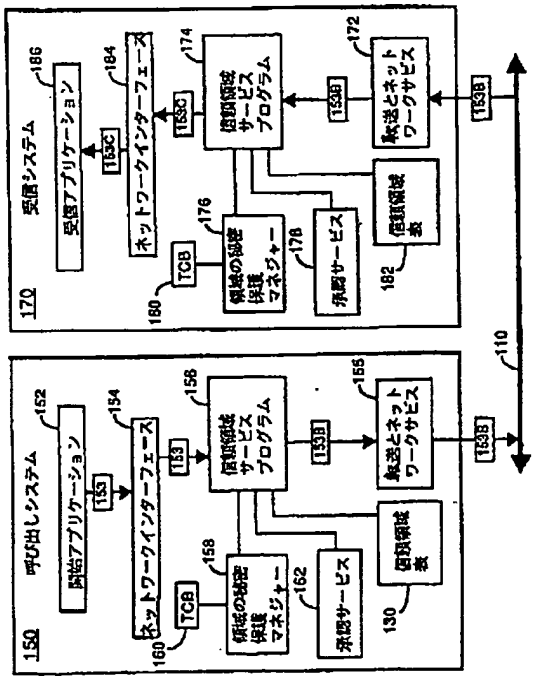
(74)代理人　弁理士　中村　稔　(外7名)

(54)【発明の名称】　分散型マルチレベル・コンピュータ機密保護システムとその方法

(57)【要約】　(修正有)

【目的】　システムの信頼領域内で行う通信を保証する機構を提供する。

【構成】　信頼領域定義表１３０，１８２はコンピュータ１５０，１７０がどの信頼領域のメンバーかを定義し、記憶したデータの機密保護のレベルを定義する。信頼領域サービス・プログラム１５６は指定したメッセージを他のコンピュータシステム１７０へ送信するために両方が共通の信頼領域のメンバーであることを検査し、プロトコル・データ・ユニットとして送信する。受信システム１７０はそのデータ・ユニットの成分を検証し、このメッセージに関してどの機密保護ポリシーを実行すべきかを判断する。



1

【特許請求の範囲】

【請求項1】　コンピュータ・ネットワークに接続された複数のコンピュータを有する上記のコンピュータ・ネットワークのメッセージ送信装置において、上記のメッセージ送信装置は；上記のコンピュータのいずれが所定の信頼領域のメンバーであるかを指定する情報を記憶する信頼領域定義手段によって構成され、各所定の信頼領域の全てのメンバーは共通の組の機密保護プロトコルを実行してデータの機密性を保護し；上記の複数のコンピュータの各々の機密保護装置は；上記のコンピュータ内で所定の機密保護を実行し、これに記憶した各組のデータに対して機密保護レベルを定義する委任計算基地；上記のネットワークを介して他のコンピュータに送られるメッセージを承認し検証する承認手段；上記の委任計算基地がどのようにして上記のメッセージに関する機密保護ポリシーを実行するかを指定する関連したレベルを有するデータによって構成される上記の各メッセージ；上記の委任計算基地、承認手段、および信頼領域定義手段に接続されて指定された他のコンピュータ・システムに指定されたメッセージを送信する準備を行う信頼領域サービス手段であって、上記の信頼領域定義手段によって記憶された信頼領域情報を獲得し、上記のコンピュータ・システムと上記の指定されたコンピュータ・システムの両方が少なくとも1つの共通の信頼領域のメンバーであることを検証し、上記の少なくとも1つの共通の信頼領域の中から1つの信頼領域を選択する手段；上記のコンピュータに対する識別子を承認し、上記のメッセージ、上記のメッセージと関連する上記のラベル、および上記の選択した信頼領域に対する識別子をシールする手段；および上記のコンピュータに対する上記の承認した識別子、上記のシールしたメッセージ、上記のメッセージと関連する上記のラベル、および上記の選択した信頼領域に対する上記の識別子を含むプロトコル・データ・ユニットを上記の指定された他のコンピュータに送信する手段を有する上記の信頼領域サービス手段；によって構成され、上記の信頼領域サービス手段は、上記のネットワークを介して上記のコンピュータの内の他のコンピュータによって送信されるプロトコル・データ・ユニットを受信する手段、および上記のプロトコル・データ・ユニット内の上記のシールされたメッセージを承認されたものとして受け入れる前に、上記の受信したプロトコル・データ・ユニットの上記の成分の各々を検証する手段を有する上記のコンピュータによって受信されたメッセージを検証する手段をさらに有することを特徴とするメッセージ送信装置。

【請求項2】　上記の信頼領域サービス手段は、上記の信頼領域定義手段内に記憶された上記の情報によって、上記のコンピュータおよび上記の指定されたコンピュータが共通の信頼領域のメンバーではない場合、メッセージの送信を中断する手段によってさらに構成されることを特徴とする請求項1記載のメッセージ送信装置。

2

【請求項3】　上記の信頼領域サービス手段は、上記の受信したプロトコル・データ・ユニット内の上記のラベルを上記の委任計算基地に転送する手段を有し、その結果、上記の委任計算基地が上記のラベルにしたがって上記の受信したプロトコル・データ・ユニット内の上記のメッセージに関する所定の機密保護ポリシーを実行することを特徴とする請求項1記載のメッセージ送信装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、一般的に分散型コンピュータ・システムまたはネットワークの安全性を保持することに関し、さらに詳しくは、分散型システムでコンピュータを相互に接続している物理的媒体が安全でない場合に、安全性を保持する方法とシステムに関する。

【0002】

【従来の技術】分散型コンピュータ・システムまたはネットワークで安全性を保持することは、歴史的に問題であった。この種のシステムの機密保護は幾つかの特徴を有し、これには、1通信に関わるユーザーとシステムの識別の承認、2情報の安全な伝達、および3機密通信を受信するシステムとユーザーは、通信される情報の機密性を保護するように、所定のプロコトルに従う必要があることが含まれる。多くの軍事用コンピュータ・システムでは、機密保護はコンピュータを相互接続するのに使用する通信線を含め、コンピュータ・ハードウェア全てを検査することによって保証される。しかし、大半の民生用の場合は、物理的に安全なコンピュータ・ハードウェアと通信線は現実的ではない。したがって、物理的な機密保護以外の機構を使用して、これらの民生用の用途に対して機密保護を提供しなければならない。分散型ネットワークのユーザー（実際にはメンバーと呼ばれる）に信頼できる承認を与える一般的に利用可能な技術は、ＲＳＡの公共キーによる承認、およびニーダムとシュローダ（Ｎｅｅｄｈａｍ&Ｓｃｈｒｏｅｄｅｒ）の信頼性のある第三者による承認技術［ＭＩＴの商標であり、ＭＩＴのアテナ計画によるカーベロス（ｋｅｒｂｅｒｏｓ）で使用される］を含め多数存在する。

【0003】しかし、多くのコンピュータを使用する環境では、指定されたデータに対するアクセスを許可するかどうかの決定には、ユーザーの識別情報だけでは十分とはいえない。多くの場合、この決定を行うためには、別の情報を追加する必要がある。この別の情報は、ユーザーのワークステーションの所在は何処か（例えば、安全な地区にあるか）とか、現時点でユーザーはどの機密保護レベルで稼働中かというような多くの形態を取ることが可能である。この別の情報を、ユーザーが稼働している「環境」と呼ぶ。例えば、軍需用または民生用コンピュータ・システムは、いずれも機密保護の「レベル」という概念を使用する。基本的に、多くのシステムで、

多数の個別の機密保護レベルが必要であるが、その理由は、情報の中には、他の情報より機密性が高く、機密情報の各組はこれと関連する許可された受取人の組を有するものもあるからである。

【0004】通信に加入しているユーザーは、これらユーザーが稼働している環境を常に正しく表わすと信頼されているとは限らない。その代わり、安全な通信が要求していることは、ユーザーの処理をサポートするコンピュータ稼働システムが、ネットワーク内の他のシステムに対するユーザーの環境に関する通信情報について責任を持たなければならないことである。

【0005】本発明は、システムの「信頼領域」（ｔｒｕｓｔ　ｒｅｒｌｍｓ）内で生じる通信を保証する機構を提供することによって、またシステムと通信に加入しているユーザーの両方を承認することによって、システム間に安全な通信を提供する。さらに、機密保護の複数のレベルは、指定された機密保護レベルのラベルが承認できることを受取人が検査できるようにこれらのラベルをコード化し、送信されるデータと共に、検証された機密保護レベルのラベルを送信することによってサポートされる。

【0006】

【課題を解決する手段】要約すると、本発明は、盗聴者に対して物理的に安全ではないネットワークを使用して、メッセージを交換するコンピュータ間の信頼に対する基礎を強化するコンピュータ機密保護システムである。これを行うために、本発明は、どのコンピュータが所定の信頼領域のメンバーであるかを定義する信頼領域表を設ける。各々の所定の信頼領域のメンバーの全ては、データの機密性を保護するために、共通の機密保護プロトコルのセットを実行する。

【0007】信頼領域のメンバーである各コンピュータは、所定の機密保護手段を実行し、またこのコンピュータに記憶したデータの各々に対して機密保護レベルを定義する。したがって、各メッセージは、関連するラベルを有し、このラベルはこのメッセージに対してコンピュータの機密保護ポリシーをどのように実行するかを指示する。

【0008】各コンピュータ内の信頼領域サービス・プログラムは、指定された他のコンピュータ・システムに送信するためにユーザーのメッセージにラベルを付け、これをフォーマット化する仕事を行う。この信頼領域サービス・プログラムは、コンピュータの核すなわちオペレーティング・システムの一部であり、ユーザーが自己のコンピュータが共有する信頼領域のメンバーでない他のコンピュータにデータを送信しようと試みてこのコンピュータ・システムの機密保護手段を突破しようとしない限り、通常はシステムのユーザーには分からない。指定されたメッセージを送信する前に、信頼領域サービス・プログラムは、信頼領域表を使用して、ローカル・コンピュータ・システムと指定されたターゲットコンピュータ・システムの両方が少なくとも１つの共通する信頼領域のメンバーであることを検査し、そこでそのような共通信頼領域の１つを選択する。もし、コンピュータ・システムと指定されたコンピュータ・システムが両方ともこれらの少なくとも１つの共通する信頼領域のメンバーでないならば、このメッセージの送信は許可されていないので、このメッセージは送信されない。何故ならば、指定されたターゲット・コンピュータがコンピュータの機密保護ポリシーの送信を実行する権限を与えられないからである。

【0009】もし、２台のコンピュータが共通の信頼領域のメンバーであるなら、そのメッセージは、プロトコル・データ・ユニットとして送信され、これにはメッセージのシールド・バージョン（ｓｅａｌｅｄ　ｖｅｒｓｉｏｎ）、送付システムとユーザーに対する承認された識別子、そのメッセージの機密保護レベルのラベル、および選択した信頼領域に対する識別子が含まれる。

【0010】受信したプロトコル・データ・ユニットは、このプロトコル・データ・ユニット内のシールされたメッセージを本物として受け取る前に、この受け取ったプロトコル・データ・ユニットの構成要素の各々を検証することによって処理される。さらに、受信したプロトコル・データ・ユニット内の機密保護レベルのラベルは、このメッセージに対していずれの所定の機密保護ポリシーを実行するべきかを決定するために、受信コンピュータによって使用され、。

【0011】

【実施例】本発明の他の目的および特徴は、以下の詳細な説明と添付の特許請求の範囲から、図面と関連させた場合により容易に理解される。図１を参照して、本発明は、機密保護プロトコル・システム、すなわち機密保護プロトコル技術であり、一般的にこれは狭域または広域情報通信網１１０、または他の通信媒体によって相互に接続されたコンピュータ１０２－１０８の集合１００の文脈（ｃｏｎｔｅｘｔ）内で動作する。これらのコンピュータ１０２－１０８の各々は、ネットワークされたコンピュータ・システム１００の個別のノードに位置するという。

【0012】コンピュータ１０２－１０８は各々は、標準的なコンピュータ・システムの構成部品を有し、これにはデータ処理装置、システム・バス・ランダム・アクセス・メモリＲＡＭ・リード・オンリ・メモリ（ＲＯＭ）、大型記憶装置（例えば、磁気ディスクまたは光ディスク）、ユーザー・インタフェース（例えば、キーボード、モニタおよびプリンタ）および通信ポートが含まれる。これらの物理的なコンピュータの構成部品（図示せず）は本発明によって変形されず、したがってここでは詳細に説明しない。

【0013】本発明の好適な一実施例で使用する１つの

5

特徴は、安全な「名付けサービス」（ｎａｍｉｎｇ　ｓｅｒｖｉｃｅ）１１２であり、これはネットワークを介して全てのコンピュータ１０２－１０８にアクセスすることができる。この名付けサービス１１２は、基本的に簡単なデータベース管理システムであり、これはネットワーク１１２の全てのユーザーによって正確であると信頼される１組のデータを保持する。本発明の文脈では、名付けサービス１１２は、「信頼領域」のリストを含み、これの意味は以下でより詳細に説明する。この名付けサービス１１２が安全であるといわれるのは、その文脈（およびそれの引渡し）が許可されていないソースによる変形から保護されているからであり、名付けサービス１１２からのデータの受取人は、これから得た情報が信頼できるということを知ることができる。安全な名付けサービスの構成に関わる実際上の問題が多数存在し、したがって本発明の他の実施例は信頼領域を指定するために代替の構成を使用する。

信頼領域

本発明で使用する中心概念は、「信頼領域」の概念である。信頼領域はコンピュータ・システムの集合であり、これらのコンピュータ・システムは共通の機密保護ポリシーを共有し、互いに信用あってこのポリシーを維持している。さらに、信頼領域のメンバーであるコンピュータ・システムは、システム間を送信されるメッセージの各々に関連する「環境ラベル」すなわち「機密保護レベルのラベル」を通信する方法に同意している。

【００１４】基本的に、信頼領域は、既知の組のコンピュータであり、これらのコンピュータは機密情報を正しく取り扱い、この種のデータを取り扱うための所定の組の規則に従う点で信頼することができる。一台のコンピュータでも、複数の個別の信頼領域のメンバーになることができる。２つ以上の信頼領域を有する理由は、種々の異なったコンピュータにデータを送信する場合、コンピュータ・システムは異なった機密保護ポリシーを使用することができるためである。より単純にいえば、異なった組織は機密情報を取り扱うために異なった機密保護ポリシーを使用する傾向があり、この種の機密保護ポリシーの各々に対して１つの信頼領域が存在する。例えば、軍事組織は、データを異なった機密保護レベルに組織する可能性があり、これには「取扱注意」、「秘密」、「極秘」等が含まれる。一方、産業組織は、データを「役員専用」、「重役会専用」、「管理職用情報」、「全従業員用情報」、「特別計画Ａ」等のような機密保護レベルに組織するかもしれない。各々の機密保護ポリシーは、特定の機密保護レベルのラベルをラベルを付けられたデータがどのように扱われるべきかを定義し、したがって各々の機密保護ポリシーに対して所定の組の機密保護レベルのラベルが存在する。

【００１５】図２を参照して、名付けサービス１１２は信頼領域の定義したリストを保持する。このリストは、

6

フラット・ファイルすなわちデータベース表１３０として組織され、少なくとも１つの信頼領域のメンバーである各コンピュータ・システムに対して１つの行１３２を有する。特定の指定されたコンピュータ・システムに対する行すなわち記録は、そのシステムが所属する信頼領域を全てリストする。この表１３０の好適な実施例は２つある。

【００１６】図１に示す実施例では、機密保護名付けサービス１１２があり、これには、信頼領域表１３０が含まれる。この実施例の利点は、信頼領域の保持に従事する機密保護マネジャが信頼領域表１３０の複写を１つだけ記憶する必要しかない点であり、この複写は全員が使用することに利用できる。欠点は、機密保護名付けサービスの設計が難しい点である。信頼領域表１３０の第２実施例は、少なくとも１つの信頼領域のメンバーであるコンピュータ・システムの全ての表の複写を単純に有している。これは、この表の更新事項はこれらのコンピュータ・システム全てにとって安全で確実な方法で複写されなければならないという明らかな欠点を有する。しかし、この第２実施例は、実行が比較的容易であるという利点を有する。

用語集

以下に示すのは、ここで使用される用語の定義である。

アソシエーション

本発明が呼び出したユーザーと呼び出されたユーザーを記述する承認情報、信頼領域情報、および環境情報の交換に成功した場合、アソシエーションが２台のコンピュータの間に形成される。２つのシステムが２人のユーザー間で共用されている環境を記述する共通の機密保護の文脈を形成することが、この交換によって可能になる。このアソシエーションは、これらのユーザーの間で何か別のメッセージを送った場合、送った側のユーザーとこのユーザーの環境全体を再び再承認するのではなく、送った側のシステムが以前に確立された機密保護文脈を参照することを可能にする。

承認されたメッセージ

承認されたデータとは、データの発信源（すなわち、送り主）を検証することができる承認技術を使用して暗号化または符号付け（ｓｉｇｎｅｄ）されたデータである。メッセージの「符号付け」（すなわち、データの組）は、符号が符号付けした文書（すなわちデータの組）の承認を検証するという点で、物理的に文字に符号付けするかまたはチェックすることと同様である。コンピュータ・システム内のデジタル・メッセージに符号を付けることは承認技術を使用して実行され、従来技術のコンピュータ・シテステムでこれらの多数の技術が使用され、種々の方式のデータ送信を検証している。本発明の文脈では、メッセージとこのメッセージと共に送られる関連する情報（送信システムおよびユーザー識別子、信頼領域識別子、並びにラベル）は、受信したデータが

本当に意図した送信システムによって送られたものかどうかを受信システムが検査できるように全て承認される。メッセージまたは他の組のデータの発信源は、デジタル符号をつけるか、または予め確立した発信源のみによって共有されるキーを使用してメッセージを暗号化するかのいずれかによって承認することができる。データの承認、符号付け、暗号化および復号化の詳細はここでは述べないが、その理由は、これらのテーマは当業者に周知であるからである。これらの従来技術による方法は、本発明の信頼領域機密保護方法論の一部を実行するために、本発明によって道具として使用される。

環境とラベル

内部的な機密保護を有している大部分の市販のコンピュータ・システムでは、このコンピュータに記憶されたすべてのデータは、いわゆる「環境」情報をタッグを付けられている、すなわちラベルを付けられ、これはそのデータを作り出したコンピュータ内の処理の機密保護特性を表わす。本明細書では、「機密保護レベル」と「環境」という用語は互換的に使用され、いずれもそのコンピュータによって使用される1つまたは複数の機密保護ポリシーに関係するユーザーの特性を言及するものである。

ターゲット

ターゲット・システム、すなわちターゲットのアプリケーションとは、呼び出したシステムすなわちユーザーによって通信が向けられるシステムすなわちアプリケーションである。

機密保護ポリシー

機密保護ポリシーとは、個々のコンピュータおよび（または）ユーザーに対するデータの使用可能性を決定する1組の規則であり、これには、特定のコンピュータまたはユーザーがデータにアクセスすることを認めるか拒否するかの場合に取るべきアクションの規則が付随している。多くの場合、これらの規則は、データが送られているコンピュータおよびユーザーの識別以外の要素によって決まる。特に、送信されるデータと関連する環境または機密保護レベルのラベルによって、しばしばこの送信されたデータをどのように取り扱うかが決まる。

メッセージの取扱い

図3を参照して、本発明が動作する基本的な状況は、以下の通りである。ここでは呼び出しシステムと呼ぶ第1コンピュータ１５０で稼働しているユーザーは、ここではターゲット・システムすなわち受信システムと呼ぶ特定の第2コンピュータで稼働中の特定のユーザーにメッセージを送ることを希望する。図3は、このメッセージの送信に関わる種々のソフトウエア・モジュールを示す。これらのソフトウエア・モジュールは機密保護機構を有し、これは、このメッセージの送信が許可されているかどうか、どのようにメッセージをコード化するべきであるか、およびこのメッセージの送信中並びにメッセージの受信後、どのような機密保護プロトコルを使用すべきであるかを決定する。

【００１７】図3のブロック図および図4のフロー・チャートを参照して、呼び出しシステム１５０内の開始アプリケーション１５２がメッセージ１５３を発生し、このメッセージは特定のコンピュータで稼働中の特定のユーザー（またはアプリケーション・プログラム）に送られるべきであるという命令と共にこのメッセージ１５３を呼び出しシステムのネットワーク・インタフェース１５４に送る場合に、送信プロセスは開始される（図4のステップ２００）。このネットワーク・インタフェース１５４は、潜在的に信頼されないユーザー・プログラムとこのコンピュータ・システムとの信頼されているネットワーク・プログラムとの間の境界である。

【００１８】もし呼び出しコンピュータ・システム１５０が、このコンピュータ１５０と授受されるメッセージの流れを制御するための機密保護機構を持たないならば、ネットワーク・インタフェース１５４はメッセージ１５３を直接コンピュータの転送サービス・ルーチン１５５に送り、このルーチンはネットワーク上での実際のデータの送信を取り扱う。この転送サービス・ルーチン１５５は、インターネット（Ｉｎｔｅｒｎｅｔ）のＴＣＰまたはＵＤＰ、ＩＳＯの結合指向転送サービスまたは結合なしの転送サービス（ＩＳＯ′ｓ Ｃｏｎｎｅｃｔｉｏｎ Ｏｒｉｅｎｔｅｄ ｏｒ Ｃｏｎｎｅｃｔｉｏｎｌｅｓｓ Ｔｒａｎｓｐｏｒｔ Ｓｅｒｖｉｃｅｓ）のような方式、またはどのような下層ネットワーク化プロトコル・スタックが使用されても、特定の方式のネットワーク上を送信されるデータに関連するプロトコルを取り扱う。この種のネットワークの各々は、メッセージを特定の着信局に送信することに成功するための所定のシーケンスの動作を有し、このプロトコルの詳細は転送サービス・ルーチン１５５によって取り扱われる。

【００１９】本発明の幾つかの実施例の中には、「クラス分けしないデータ」を特に設けたものがあり、このデータは、コンピュータの内部機密保護システムが機密保護プロコトルによって制約されないことを示すデータである。もし、呼び出しコンピュータシステム１５０がこの種のデータを有し、送信されているメッセージがクラス分けされないならば（ステップ２０２）、このメッセージは、それ以上の処理を行わずに送信される（ステップ２０４）。本発明の他の実施例では、「クラス分けしないデータ」の特別な取り扱いは行われないが、その理由は、当該コンピュータ・ネットワークのコンピュータ・システムは、送信されたデータが全て機密であるとして取り扱う必要があり、または少なくとも関連するデータ機密保護レベルを有するものとして取り扱う必要があるからである。

【００２０】このメッセージが機密保護の目的のためにクラス分けされるか、または呼び出しシステムがクラス

分けされないデータ、現在信用されているかまたは保護されているメッセージ１５３を持たないかのいずれかであると仮定すると、次にコンピュータ・システムの一部が信頼領域サービス・プログラム（ＴＲＳＰ）１５６によって処理される。このＴＲＳＰの最初の仕事は、呼び出しシステムとターゲット・システムの両方が、共有信頼領域のメンバーであるかどうかを決定することである（ステップ２０６および２０８）。これは、信頼領域表１３０から、（１）ターゲット・システムに関連する信頼領域の組、および（２）呼び出しシステムに関連する信頼領域の組を取り出すことによって行われる。もしこのターゲット・システムが信頼領域表１３０にリストされていないならば、これはいずれの信頼領域のメンバーでもないことを意味することに留意すること。２つのシステムがいずれも共通の信頼領域のメンバーではないならば（または、別の言い方では、もしターゲット・システムが、呼び出しシステムがメンバーであるいずれの信頼領域のメンバーでもないならば）、このメッセージ送信シーケンスは中断され、このメッセージは送られない（ステップ２１０）。基本的に、２つのシステムに対して共通の信頼領域が存在しないならば、メッセージの送信は許可されず、したがってこのメッセージは送信されない。

【００２１】次に、ＴＲＳＰ１５６は、呼び出しシステムとターゲット・システムの両方がメンバーである信頼領域の組の中から信頼領域を選択しなければならない（ステップ２１２）。もし共通の信頼領域が１つのみ存在するならば、そこでこれが選択され、それ以外の場合には、信頼領域の内の１つを選択しなければならない。この選択を行う方法は、機密保護の考え方に依存し本発明には関係ないが、一般的に信頼領域は、２つ以上の共通信頼領域が存在する場合どれを選択するべきかという点から優先順位をつけられるか、または信頼領域の選択が、送られているメッセージの特性によって決められるかのいずれかである。一度信頼領域が選択されると、ＴＲＳＰ１５６は選択された信頼領域の機密保護管理プログラム１５８を呼びだす。

【００２２】信頼領域機密保護管理プログラム１５８は、特定の信頼領域の機密保護ポリシーを実行することに責任を負うプログラムである。このプログラムは、この信頼領域に対する所定の組の規則にしたがって、データ機密保護レベルのラベルを取扱い、委任された（ｔｒｕｓｔｅｄ）計算基地１６０と対話を行って、送られているメッセージと関係のあるローカル・データ機密保護レベルのラベルを得る。このプログラムは、また受信したメッセージのデータ機密保護レベルのラベルが、このコンピュータのローカル・データ機密保護レベルのラベルに関連したフォーマットに変換して戻せるように、委任された計算基地１６０と対話を行う。

【００２３】委任された計算基地１６０は、コンピュータのローカル機密保護ポリシーを保持する責任のあるコンピュータ・システムの部分である。これは、システムに記憶されたデータの機密性を保持し、許可されないデータがユーザーとコンピュータ上で実行される処理との間で共有されることを防止することを意味する。したがって、この委任された計算基地１６０は、コンピュータ上で実行される処理とその処理によって作られまたは記憶されるデータに対して、機密保護レベルのラベルまたは環境情報を割り当てる責任がある。

【００２４】次に、信頼領域機密保護管理プログラム１５８は、委任された計算基地（ＴＣＢ）１６０を呼び出して開始アプリケーション１５２に関連する（すなわち、送信されているメッセージに関連する）環境またはデータ機密保護レベルのラベルを決定する。多数の異なった方式のコンピュータが信頼領域を共有し、ローカル・データ機密保護レベルのラベルを示すのに使用される内部フォーマットは信頼領域内のコンピュータによって変化する可能性があることに留意すること。したがって、もし必要なら、信頼領域機密保護管理プログラム１５８は、呼び出しコンピュータ１５０によって使用されるローカル・データ機密保護レベルのラベルをデータ機密保護レベルのラベル送信するために信頼領域によって使用されている他のフォーマットに変換する（ステップ２１４）。もしＴＣＢ１６０がメッセージ１５３を送信することを許可するなら（ステップ２１６）、に次に、この許可と新しいフォーマット・ラベルはＴＲＳＰ１５５に戻される。それ以外は、許可は否定され、このメッセージ送信シーケンスは中断され、このメッセージは送信されない（ステップ２１０）。信頼領域機密保護管理プログラム１５８は、また通常ローカルＴＣＢ１６０によって実行されない信頼領域が必要とする全てのチェックを実行する。

【００２５】ＴＣＢ１６０からメッセージを送る許可が得られたと仮定すると、送信されるメッセージは、呼び出しシステムとユーザーに対する承認された識別子、信頼領域を有するように、また機密保護レベルのラベルも有するように、新しいフォーマットに変換される（ステップ２１８）。その後の次のステップは、受信システム１７０が受信したメッセージを検証できるように、メッセージを承認することである（ステップ２２０）。さらに詳しくは、呼び出しシステムとユーザーが承認され、信頼領域識別子と機密保護レベルのラベルがシステムの承認の下で符号付けされ、ユーザーメッセージがユーザーの承認の下で符号付けされる。承認と符号付けは、信頼領域サービス・プログラム１５６が承認サービス・プログラム１６２を呼ぶことによって実行され、承認サービス・プログラム１６２は、符号付けしたデータの発信源を検証するように、データの指定した組を符号付けする。実施例の中には、符号付けしたデータを暗号化し、その結果、ネットワーク・トラフィックを監視する盗聴

者が、送信されているメッセージの内容を判別できないようにするものもある。

【００２６】図６に示すその結果生じる送信されるメッセージ１５３Ｂに対するデータの構成は、呼び出しコンピュータの転送サービス・モジュール１５５に送られ、通信ネットワーク１１０上をターゲット・コンピュータ・システム１７０に送信される（ステップ２２２）。図６に示すデータ構成は、一般にプロトコル・データ・ユニットとして知られ、プロトコル制御情報２５１を有し、これには使用中の信頼領域２５２、信頼領域２５４に関連するフォーマット内で指定されるデータ機密保護レベルのラベル２５４、および受信コンピュータ・システムでデータを取り扱う場合に使用されるプロトコルを特定するのに必要な他の全ての情報２５６が含まれる（これらは全て符号付けされた値である）。この情報は「シールされ」るが、このことは、これが承認サービス・プログラム１６２を使用して暗号化されるかまたは符号付けされるかのいずれかであることを意味する。呼び出しシステム２６２とユーザー２６６に対する承認情報２６２もまた存在する可能性がある。２つのコンピュータ・システム間でアソシエーションが確立した場合、この情報は、既存のアソシエーション２５７に照会を送ることによって、およびもし必要なら、このアソシエーションが確立してから変化した機密保護レベルのラベル２５８の特徴も送ることによって、短縮化（ａｂｂｒｅｖｉａｔｅ）することができる。メッセージ・データ構成は、またサービス・データ・ユニット２６０を有し、これにはユーザーの「シールされたメッセージ」２６８（すなわち、暗号化されたか、または符号を付けたメッセージ）が含まれる。

【００２７】図５を参照して、送信されたメッセージが受信システム１７０で受信された場合（ステップ２３０）、受信されたメッセージ１５３Ｂは、以下のように処理される。信頼領域機密保護プロトコルの範囲外で送信されたクラス分けされていないメッセージは、そのように認識され（ステップ２３２）、信頼領域サービス・プログラム１７４によって、ネットワーク・インタフェース１８４を介して受信アプリケーション１８６に直接転送され（ステップ２３４）、以下に説明する検証ステップを実行しない。

【００２８】受信したメッセージ１５３Ｂがクラス分けされていないと仮定すれば、この受信したメッセージは、受信コンピュータの転送サービス・ルーチン１７２によって先ずそのコンピュータの信頼領域サービス・プログラム１７４に送られて検証される。信頼領域サービス・プログラム１７４は、受信システムの承認サービス・プログラム１７８を呼び出すことによってこの受信したメッセージを検証する（ステップ２３６）。

【００２９】もし、メッセージのいずれかの部分（すなわち、送信されたプロトコル・データ・ユニット）が承認サービス・プログラム１７８によって検証されないならば（ステップ２３８）、このメッセージ転送処理は中断され、受信したメッセージは廃棄される（ステップ２４０）。メッセージの検証を失敗したことは、送ったと推定される送り手がこのメッセージを送らなかったか（すなわち、これは送り出しシステムであるかのようなポーズをとる盗聴者からのメッセージである）、またはメッセージのある部分に送信処理中に盗聴者によって変更された部分があるか、のいずれかであることを意味する。

【００３０】もし送信システムまたは受信システムの識別子が検証に成功したならば、これは、推定される送信システムが実際にこのメッセージを送ったことを意味し、またこの送信システムは受信システムがターゲット・システムになることを意図したことを意味する。さらに、このメッセージに対する機密保護レベルのラベルは検証され、したがって有効であること分かる。

【００３１】次に、受信システムのＴＲＳＰ１７４は、信頼領域表１８２をチェックして、この識別された送信システムが受信したメッセージ１５３Ｂによって指定された信頼領域のメンバーであるかどうか、およびこの受信システムがまたその信頼領域にあるかどうかを判断する（ステップ２４２と２４４）。もしそうでなければ、次に、メッセージは誤って送信され、このメッセージはこのシステム１７０によって受信を許可されなかったものとして廃棄される（ステップ２４０）。

【００３２】信頼領域のチェックが成功したと仮定すると（ステップ２４４）、受信した機密保護レベルのラベルは、適当な信頼領域機密保護マネジャ１７６に転送されて、もし必要ならば、受信コンピュータの委任計算基地１８０で使用されるフォーマットに変換される（ステップ２４５）。次に、信頼領域機密保護マネジャ１７６は、ＴＣＢ１８０をチェックして、ラベルを付けられたメッセージをターゲット・アプリケーションに転送する許可を得る（ステップ２４６）。もし許可が得られなければ（ステップ２４７）、次にこのメッセージは転送されない（ステップ２４７）。それ以外は、機密保護レベルのラベルを含め、検証されたメッセージの制御は、信頼領域サービス・プログラム１７４に送り返される。

【００３３】最後に、もしメッセージがこれらの試験を全てパスしたならば、変換されたメッセージ１５３Ｃ（これは送られた元のメッセージ１５３と同一である）のメッセージ部分は、ネットワーク・インタフェース１８４を介して受信アプリケーション１８６に転送される（ステップ２４８）。

アソシエーションの確立

全ての信頼領域情報と機密保護レベルのラベル情報が検証された場合（ステップ２３６、２３８、２４２および２４４）、この情報は受信システムに記憶され、これによって送信システムのアソシエーションを確立する。こ

13

のアソシエーションが確立することによって、送信システムが、２つのシステム間で最後にメッセージが送られてから変化しないプロトコル制御情報２５１（図６参照）のこれらの部分の情報を除去することが可能になり、データをより効率的に送信することができる。さらに、アソシエーションの確立に失敗すると、自動的に受信したメッセージを拒絶する結果となるが、その理由は、受信したメッセージの承認が証明されていないからである。好適な実施例では、所定の期間の後、もし２つのシステム間でデータの送信が継続することによってアソシエーションが更新されなければ、これらのアソシエーションは自動的に終了する。

代替実施例

幾つかの特定の実施例を参照して本発明を説明したが、この説明は本発明を例示するものであって、本発明を限定する意味は持たない。添付の特許請求の範囲によって定義される本発明の真の精神と範囲から逸脱することなく、種々の変形が、当業者によっておこなわれる。

【図面の簡単な説明】

【図１】多数の独立したコンピュータ・システムに接続されたコンピュータ・ネットワークのブロック図である。

【図２】信頼領域表の一実施例を示す。

【図３】ネットワークによって相互に接続された２台のコンピュータのブロック図であり、これらのコンピュータの内の１台はデータを他方のコンピュータに送信している。

14

【図４】本発明の安全なデータ送信方法のフロー・チャートである。

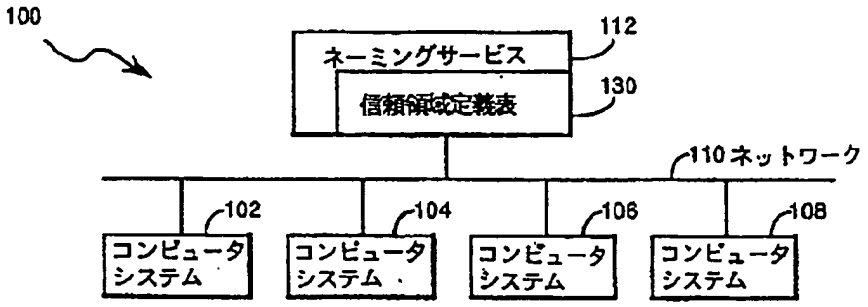
【図５】本発明の安全なデータ送信方法のフロー・チャートである。

【図６】あるコンピュータから他のコンピュータに送信されるメッセージ用のデータ構成のブロック図である。

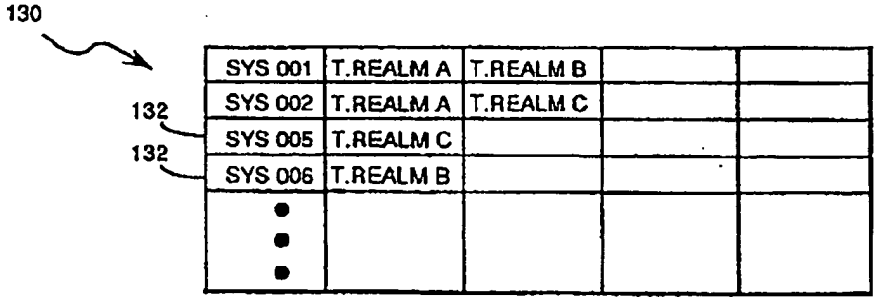
【符号の説明】

１００　コンピュータの集合
１０２－１０８　コンピュータ
１１０　狭域または広域情報通信網
１１２　名付けサービス・ネットワーク
１３０、１８２　データベース表
１５０　呼び出しシステム（第１コンピュータ）
１５２　開始アプリケーション
１５３、１５３Ｂ、１５３Ｃ　メッセージ
１５４、１８４　ネットワーク・インタフェース
１５５、１７２　転送サービス・ルーチン
１５６、１７４　信頼領域サービス・プログラム（ＴＲＳＰ）
１５８、１７６　信頼領域機密保護管理プログラム
１６０、１８０　委任された計算基地
１６２、１７８　承認サービス・プログラム
１７０　受信システム（第２システム）
１８６　受信アプリケーション

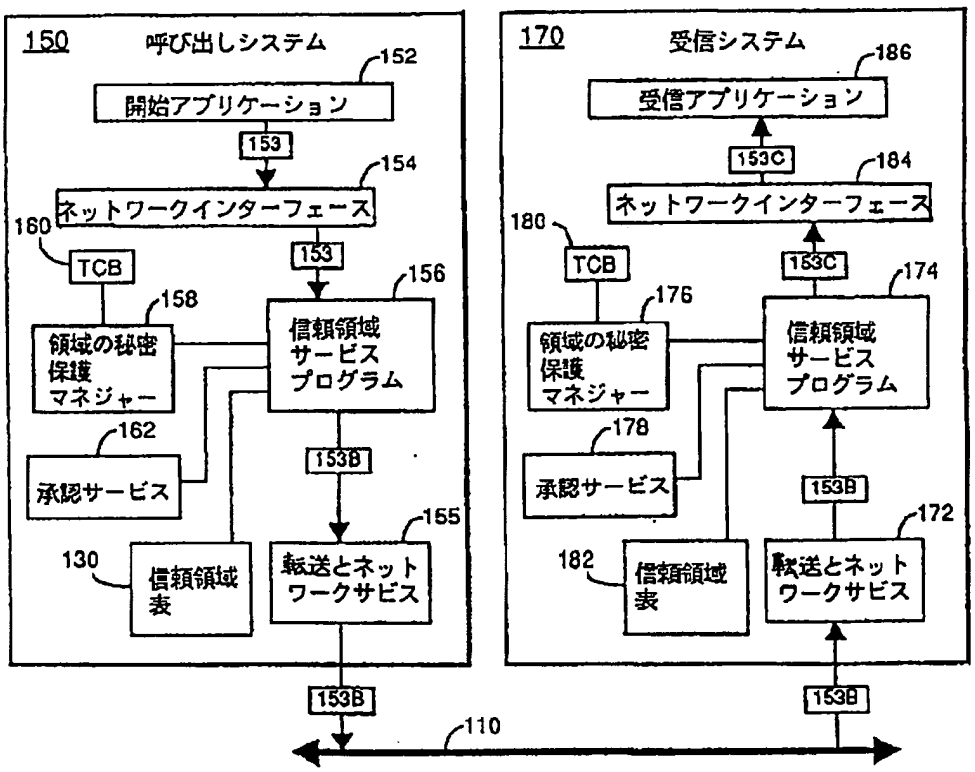
【図１】



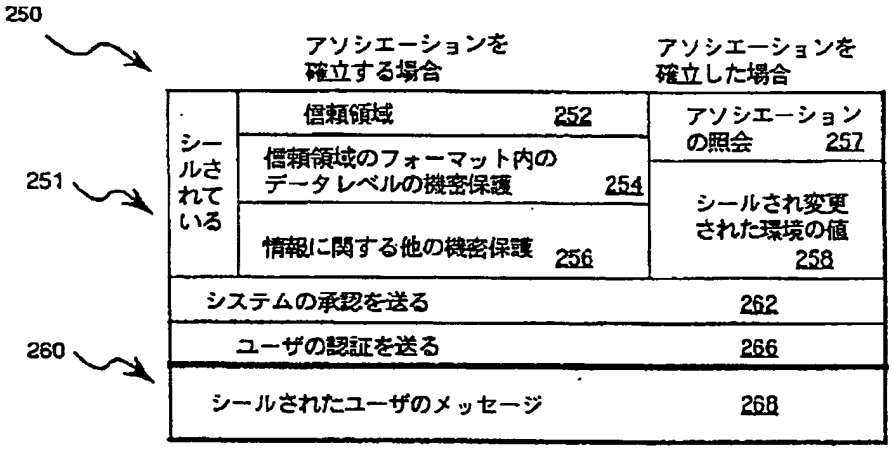
【図２】



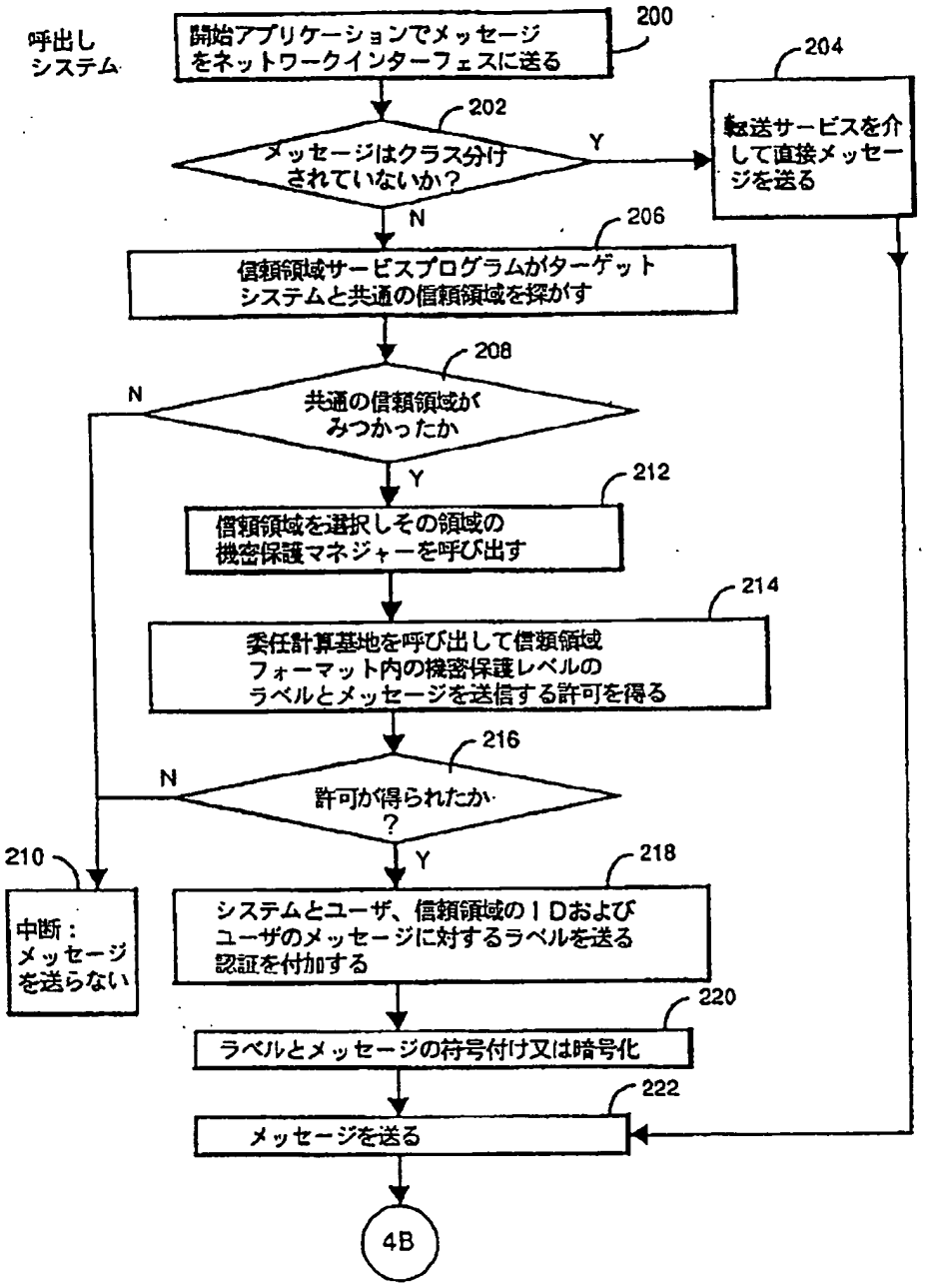
【図3】


150
呼び出しシステム
152
開始アプリケーション
153
154
ネットワークインターフェース
160
TCB
153
156
158
領域の秘密保護マネジャー
信頼領域サービスプログラム
162
承認サービス
153B
155
130
信頼領域表
転送とネットワークサビス
153B
110
170
受信システム
186
受信アプリケーション
153C
184
ネットワークインターフェース
180
TCB
153C
174
176
領域の秘密保護マネジャー
信頼領域サービスプログラム
178
承認サービス
153B
172
182
信頼領域表
転送とネットワークサビス
153B

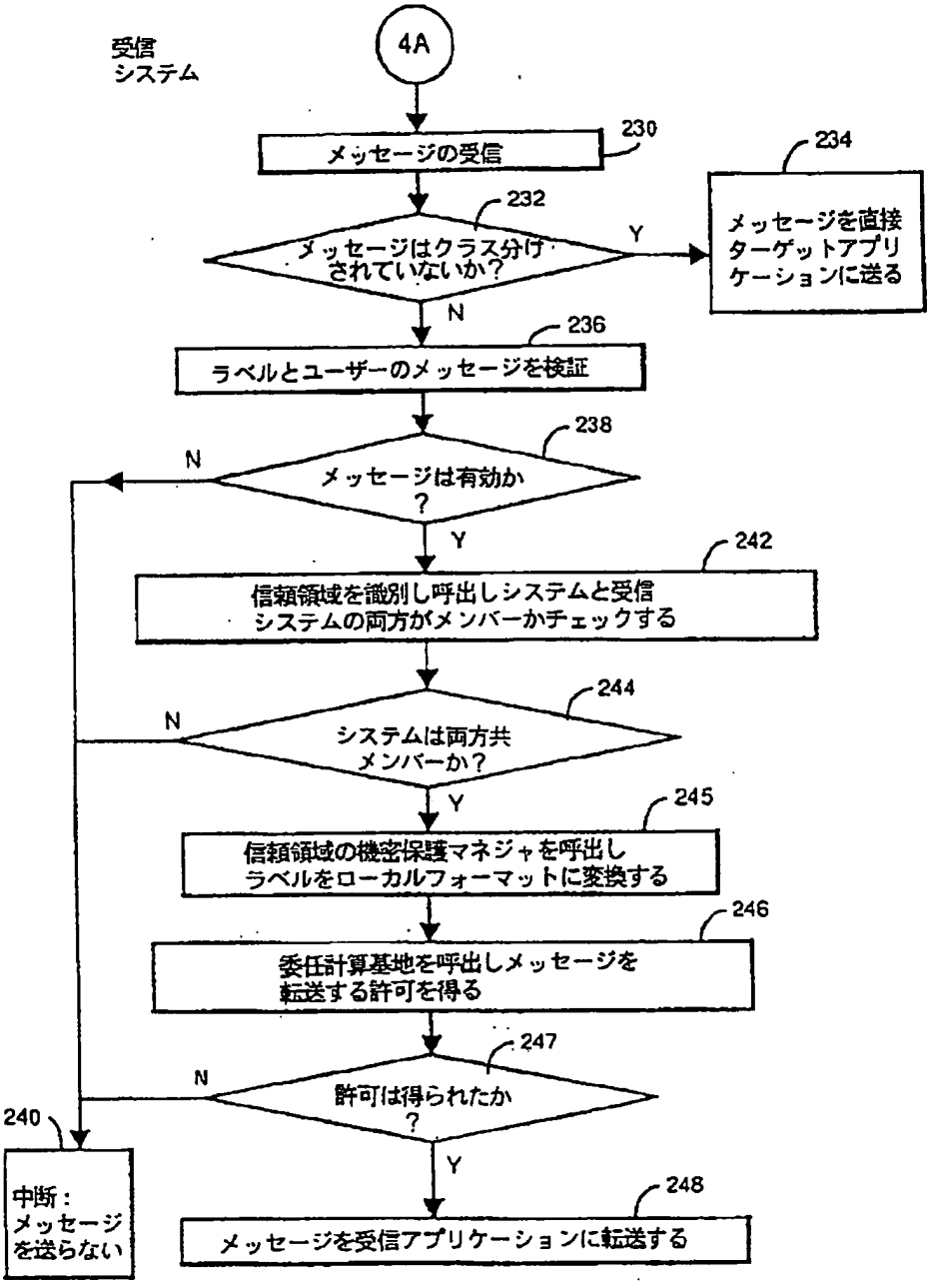
【図5】


250
アソシエーションを確立する場合
アソシエーションを確立した場合
シールされている
信頼領域 252
アソシエーションの照会 257
251
信頼領域のフォーマット内のデータレベルの機密保護 254
シールされ変更された環境の値 258
情報に関する他の機密保護 256
システムの承認を送る 262
260
ユーザの認証を送る 266
シールされたユーザのメッセージ 268

【図4】


呼出し
システム
開始アプリケーションでメッセージをネットワークインターフェスに送る
200
メッセージはクラス分けされていないか？
202
Y
N
転送サービスを介して直接メッセージを送る
204
信頼領域サービスプログラムがターゲットシステムと共通の信頼領域を探がす
206
共通の信頼領域がみつかったか
208
N
Y
信頼領域を選択しその領域の機密保護マネジャーを呼び出す
212
委任計算基地を呼び出して信頼領域フォーマット内の機密保護レベルのラベルとメッセージを送信する許可を得る
214
許可が得られたか？
216
N
Y
中断：メッセージを送らない
210
システムとユーザ、信頼領域のIDおよびユーザのメッセージに対するラベルを送る認証を付加する
218
ラベルとメッセージの符号付け又は暗号化
220
メッセージを送る
222
4B

【図6】


受信
システム
4A
メッセージの受信
230
メッセージはクラス分けされていないか?
232
Y
234
メッセージを直接ターゲットアプリケーションに送る
N
ラベルとユーザーのメッセージを検証
236
メッセージは有効か?
238
N
Y
信頼領域を識別し呼出しシステムと受信システムの両方がメンバーかチェックする
242
システムは両方共メンバーか?
244
N
Y
信頼領域の機密保護マネジャを呼出しラベルをローカルフォーマットに変換する
245
委任計算基地を呼出しメッセージを転送する許可を得る
246
許可は得られたか?
247
N
Y
240
中断:メッセージを送らない
メッセージを受信アプリケーションに転送する
248